IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation, Plaintiff-Counterdefendant, v. SECURE COMPUTING CORPORATION, a Delaware corporation, CYBERGUARD, CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100, Defendants-Counterclaimants.	C. A. No. 06-369 GMS

PLAINTIFF FINJAN SOFTWARE, LTD.'S
OPENING CLAIM CONSTRUCTION BRIEF

OF COUNSEL

Paul J. Andre
Lisa Kobialka
Meghan A. Wharton
James R. Hannah
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(650) 838-4300

Philip A. Rovner (#3215)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(303) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

Dated: September 7, 2007

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 2

A. Background of the Finjan Patents 2

B. Description of the Finjan Patents and Intrinsic Evidence 4

C. Background of the Secure Computing Patents 5

III. CONSTRUCTION OF TERMS 6

A. Applicable Law 6

B. Claim Interpretation of Finjan's '194 Patent 7

1. "Downloadable" 7

2. "addressed to a client" 10

3. "server that serves as a gateway to the client" 13

C. Claim Interpretation of Finjan's '780 Patent 14

1. "performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID" 14

D. Claim Interpretation of Finjan's '822 Patent 15

1. "downloadable-information" 15

2. "information-destination" 17

3. "information-recommunicator" 18

4. "evaluating the detection indicators" 19

5. "level of downloadable-information characteristic and executable code characteristic correspondence" 20

E. Claim Interpretation of Secure Computing's '010 Patent 21

1. "document control server" 21

2. "fetching the requested document" 24

3. "proxy" 25

4. "role" 26

F. Claim Interpretation of Secure Computing's '361 Patent 26

1. "firewall" 27

2. "a server having at least one directory that can be accessed using a network protocol" 28

3. "authorization filter" 29

4. "directory schema that is predefined by said entity" 29

5. "network protocol" 31

6. "per-service authorization scheme" 31

7. "per-user authentication scheme" 32

IV. CONCLUSION 33

TABLE OF AUTHORITIES

Cases

Bell Atlantic Network Servs., Inc. v. Covad Communs. Group, Inc.,
262 F.3d 1258 (Fed. Cir. 2001) 27
Cardiac Pacemakers, Inc. v. St. Jude Medical, Inc.,
381 F.3d 1371 (Fed. Cir. 2004) 1
Fuji Photo Film Co. v. Int'l Trade Comm.,
386 F.3d 1095 (Fed. Cir. 2004) 1
Interactive Gift Express, Inc. v. Compuserve, Inc.,
256 F.3d 1323 (Fed. Cir. 2001) 6
Iredeto Access, Inc. v. Echostar Satellite Corp.,
383 F.3d 1295 (Fed. Cir. 2004) 27
Key Pharm. v. Hercon Labs. Corp.,
161 F.3d 709 (Fed. Cir. 1998) 6
Kinik Co. v. International Trade Comm'n,
362 F.3d 1359 (Fed. Cir. 2004) 7, 25
Medrad, Inc. v. MRI Devices Corp.,
401 F.3d 1313 (Fed. Cir. 2005)) 1
Metabolite Labs., Inc. v. Laboratory Corp. of Am. Holdings,
370 F.3d 1354 (Fed. Cir. 2004) 7, 26
Microsoft Corp. v. Multi-Tech Sys., Inc.,
357 F.3d 1340 (Fed. Cir. 2004) 8
Multiform Desiccants, Inc. v. Medzam, Ltd.,
133 F.3d 1473 (Fed. Cir. 1998) 7, 22
Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 1, 6, 13, 28
Renishaw PLC v. Marposs Societa' per Azioni,
158 F.3d 1243 (Fed. Cir. 1998) 9
Scriptgen Pharms., Inc. v. 3-Dimensional Pharm., Inc.,
79 F. Supp. 2d 409 (D. Del. 1999) 6, 8
Tap Pharm. Prods., Inc. v. Owl Pharms., L.L.C.,
419 F.3d 1346 (Fed. Cir. 2005) 29
Watts v. XL Sys., Inc.,
232 F.3d 877 (Fed. Cir. 2000) 8

I. INTRODUCTION

Finjan Software Limited ("Finjan") is asserting United States Patent Nos. 6,092,194 ("the '194 Patent"), 6,804,780 ("the '780 Patent"), 7,058,822 ("the '822 Patent") (collectively "the Finjan Patents") against Defendants Secure Computing Corporation, Cyberguard Corporation, and Webwasher AG (collectively "Secure Computing"). JA1-20 ('194 Patent); JA21-38 ('780 Patent); JA39-62 ('822 Patent).[1] All of the Finjan Patents are from the same patent family and cover various steps to protect a network from malicious content. The claims of the Finjan Patents are exceptionally clear and straightforward, especially in light of the specifications and file histories, such that only 9 terms are in dispute out of the 67 claims asserted by Finjan. Of the 9 disputed terms, only 4 require construction.

Secure Computing is asserting U.S. Patent Nos. 6,357,010 ("the '010 Patent") and 7,185,361 ("the '361 Patent") (collectively "the Secure Computing Patents") against Finjan. JA63-83 ('010 Patent); JA84-93 ('361 Patent). The '010 Patent involves a system which allows business partners to access a company's internal network. The '361 Patent describes a firewall which does not use its own database to authenticate users, but rather, relies on a directory using lightweight directory access protocol ("LDAP"). Arguing that most of the disputed terms in the Secure Computing Patents are understood if afforded their ordinary meaning, Defendants are attempting to broadly construe the claims, which are specific in nature. The Court should not, however, "look at the ordinary meaning of the term . . . in a vacuum. Rather, [courts] must look at the ordinary meaning in the context of the written description and the prosecution history." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (quoting *Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed. Cir. 2005)); *see also Fuji Photo Film Co. v. Int'l Trade Comm.*, 386 F.3d 1095, 1098 (Fed. Cir. 2004) ("Claims must be read in the context of the specification of which they are a part") (citation omitted); *Cardiac Pacemakers, Inc. v. St. Jude*

---

[1] All "JA" citations are to the Joint Appendix pursuant to this Court's May 17, 2007 Oral Order, to be filed on the same day the answering claim construction briefs are filed.

Medical, Inc., 381 F.3d 1371, 1381 (Fed. Cir. 2004) ("A claim limitation is always construed in light of the specification, whatever the form of the claim") (citations omitted). Because of the particularity of the claims in light of the intrinsic evidence, 11 terms out of the 22 asserted claims require construction.

II. FACTUAL BACKGROUND

A. Background of the Finjan Patents

The Finjan Patents are pioneering in the field of behavior based network security. In a typical network security system, an external network, such as the Internet, is coupled to an internal network through a server known as a gateway. To access content on an external network, such as an Internet webpage, a user normally clicks on a link of a desired webpage using a web browser. Once the user clicks the link, a request is sent from the user's computer, or client, to the gateway. The gateway then forwards the request to a server hosting the webpage. In response, the content on the webpage is delivered to the gateway which sends the content to the client.[2] During the delivery of the webpage to the client, the gateway intercepts the response to determine whether the content of the webpage is at least in part malicious. *See, generally,* JA13-14 ('194 Patent at 2:66-3:61). The figure below illustrates this process.

The interception of the webpage by the gateway is a typical method for protecting a network from threats on the Internet. These threats are commonly referred to as viruses because they

---

[2] It should be noted that this is a highly simplified example. Normally, there are many servers and other components between the client computer and the web server which relay the user's request to the web server and the web server's response, or webpage, back to the client computer.

infect and damage the computer network in the same way that a cold or flu infects a person. Viruses come in a variety of shapes and pose a serious threat to the integrity of every computer network connected to the Internet. *See, generally,* JA13 ('194 Patent at 1:24-57); JA51 ('822 Patent at 1:25-2:10).

The traditional method for protecting a network against viruses is signature-based scanning. A signature is similar to a fingerprint in that it is used to identify a particular virus. Traditional scanners maintain a database of virus signatures and when a file is received, the file is scanned to determine whether it contains one of the signatures, or fingerprints, stored in the database. If the file contains a signature matching one in the database, the file is flagged as having a virus and appropriate measures are taken, including denying the file access to the network. *See, generally,* JA13 ('194 Patent at 1:24-57); JA51 ('822 Patent at 1:25-2:10).

Signature-based scanning, however, protects only against known viruses corresponding to identifiable signatures. When a new virus is created and unleashed onto the Internet, signature-based scanning is unable to protect the network until a new signature is developed for the virus and uploaded to the signature database. Meanwhile, between the release of the virus and the creation of the corresponding signature, the network is vulnerable to the new virus because there is no way for the scanner to detect the virus. *See, generally, id.*

For instance, several thousand viruses known today attempt to delete all the files stored on a computer. Traditionally, to prevent these viruses from deleting all the files stored on a computer, a signature must be created for each virus so that the scanner can identify and block the viruses. However, if a new virus is released that attempts to delete all the files stored on the computer, the computer will be vulnerable until a signature is created to identify the virus. *See, generally, id.*

To address this issue, the inventors of the Finjan Patents created a revolutionary invention. Rather than examining a file to determine whether it includes a virus signature, the new invention detects virus by observing the file's behavior. *See, generally,* JA13 ('194 Patent at 1:60-2:37). While each virus is written differently (and therefore requires a different

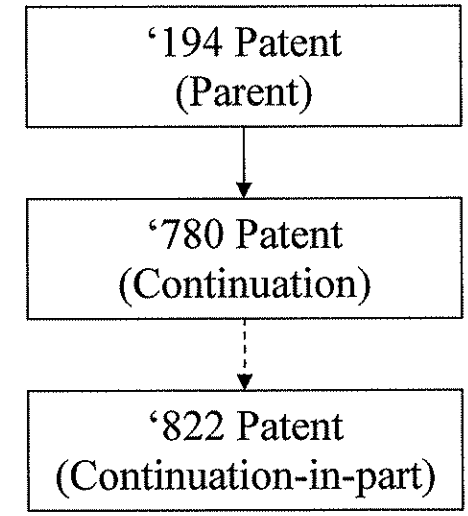
signature), the vast majority attempt similar operations. Therefore, by examining the behavior rather than detecting the signature, the computer network is protected against all viruses, whether known or unknown, that perform malicious operations. Referring again to the example set out above, a security system that analyzes the behavior of a file will determine that the received file is attempting to delete all of the files stored on the computer. Consequently, since deleting all files stored on a computer is a behavior typically associated with a virus, the security system will block the file even though the virus has not yet been identified and does not correspond to a known signature. *See, generally*, JA13 ('194 Patent at 1:24-57); JA51 ('822 Patent at 1:25-2:10).

B. Description of the Finjan Patents and Intrinsic Evidence

Finjan's '194 Patent is entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables" and discloses an innovative system for protecting a network from suspicious Downloadables based on behavior. Generally, the system includes a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. *See* JA13 ('194 Patent at 1:60-65). The Downloadable may include a Java applet, an ActiveX control, a JavaScript script, or a Visual Basic script. *Id.* ('194 Patent at 1:65-67).

The '780 Patent is a continuation of the '194 Patent, and therefore shares the same title and the same specification. The '780 Patent claims, however, are directed to methods and systems for generating a Downloadable ID. By generating an identification for each examined Downloadable, the invention allows the Downloadable to be recognized without reevaluation. Such recognition increases efficiency while also saving valuable resources, such as memory and computing power.

The '822 Patent is entitled "Malicious Mobile Code Runtime Monitoring System and Methods" and is a continuation-in-part application of the '780 Patent which, as stated above, is a continuation application based on the '194 Patent. The relationship between the Finjan Patents is illustrated graphically below:



→ = Continuation application, substantially identical specification

⇢ = Continuation-in-part, similar specification

As described previously, the invention of the '194 Patent analyzes and blocks the Downloadable at the gateway if it violates a security policy. The '780 Patent, in turn, discloses an invention for creating a Downloadable ID for each Downloadable examined at the gateway. The '822 Patent extends the '194 and the '780 Patents by wrapping a suspicious Downloadable in what is known as a "sandbox" and delivering the sandbox to the client. *See* JA51-52 ('822 Patent at 2:17-4:41). Much like sandboxes that are designed to keep children confined to a protected play area, the sandbox in this context provides a monitoring mechanism that continuously protects the network against malicious code. If malicious code is executed that was not detected at the gateway, the sandbox will trap the malicious code to neutralize its harmful effects.

C. Background of the Secure Computing Patents

As evidenced by the claim language, the Secure Computing Patents disclose very specific technical inventions. The '010 Patent is directed at a system that allows external business partners to view documents on another company's internal, non-public network. *See* JA72 ('010

Patent at 1:12-2:30). The system allows such access with "a go-list processor for determining if the user has authorization to access [the] documents," where a "go-list" is "a list which is unique to each role and used by the document control server to determine which documents an authenticated business partner may be allowed to display." JA80 ('010 Patent at 17:3-19); Final Joint Claim Construction Chart (Docket Entry No. 108). In addition, the '010 Patent discloses a similar method for "limiting access from an external network to documents stored on an internal network" that requires "a document list naming document available to clients assigned to the client's role." JA79 ('010 Patent at 16:29-44).

Secure Computing's '361 Patent describes a particular type of firewall used by a company to protect its internal network resources from unauthorized users. *See* JA91 ('361 Patent at 3:3-19). Typically, a firewall is installed at the gateway and uses its own authentication database to verify whether a particular user can access a resource on the internal network. *See* JA90 ('361 Patent at 1:14-43). Rather than having its own database, the firewall disclosed in the '361 Patent uses information stored in a lightweight directory access protocol (LDAP) directory server. *See* JA91 ('361 Patent at 4:41-44).

III. CONSTRUCTION OF TERMS

A. Applicable Law

To construe claim terms of a patent, it is well-settled that the Court looks first to the intrinsic evidence, i.e., the patent's claims, specification, and prosecution history. *See Phillips*, 415 F.3d at1312. If the Court is able to ascertain an unambiguous meaning for a claim term after examining only the intrinsic evidence, claim construction is complete. *Interactive Gift Express, Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1332 (Fed. Cir. 2001). In other words, "if the meaning of a disputed claim term is clear from the intrinsic evidence, that meaning and no other must prevail; it cannot be altered or superseded by expert witness testimony or other external sources simply because one of the parties wishes it were otherwise." *Scriptgen Pharms., Inc. v. 3-Dimensional Pharm., Inc.*, 79 F. Supp. 2d 409, 411 (D. Del. 1999) (quoting *Key Pharm. v. Hercon Labs. Corp.*, 161 F.3d 709, 716 (Fed. Cir. 1998) (citations omitted)). In specific

instances where undefined technical terms appear in the claims, the Federal Circuit has consistently encouraged the courts to look to the specification and the prosecution history for guidance. *See, e.g.*, *Metabolite Labs., Inc. v. Laboratory Corp. of Am. Holdings*, 370 F.3d 1354, 1360 (Fed. Cir. 2004), *cert. dismissed*, 126 S.Ct. 2921 (2006) ("In most cases, the best source for discerning the proper context of claim terms is the patent specification wherein the patent applicant describes the invention. In addition to providing contemporaneous technological context for defining claim terms, the patent applicant may also define a claim term in the specification 'in a manner inconsistent with its ordinary meaning.'") (citations omitted); *Kinik Co. v. International Trade Comm'n*, 362 F.3d 1359, 1365 (Fed. Cir. 2004) ("The words of patent claims have the meaning and scope with which they are used in the specification and the prosecution history.") (citation omitted); *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1478 (Fed. Cir. 1998) ("The best source for understanding a technical term is the specification from which it arose, informed, as needed, by the prosecution history.")

B. Claim Interpretation of Finjan's '194 Patent

As a result of the parties' meet and confer efforts, there are now three terms at issue for the '194 Patent. Finjan contends that only the term "Downloadable" requires construction, as the ordinary meaning within the context of the claims applies to the remaining two terms, "addressed to a client" and "server that serves as a gateway to the client."

1. "Downloadable"

Finjan's Construction	Secure Computing's Construction
program or document containing mobile code	a program or document containing an executable application program that can be downloaded from one computer to another computer

"Downloadable" is prominently featured in the '194 Patent, entitled "System and Method for Protecting a Computer and Network from Hostile Downloadables," and appears in every claim. Finjan's construction of "program or document containing mobile code" finds substantial support in the intrinsic evidence. In particular, the '194 Patent specification states that "[a] Downloadable is an executable application program, which is downloaded from a source

computer and run on the destination computer." JA13 ('194 Patent at 1:44-47). During the prosecution of the '194 Patent, the patent applicant expounded on this statement and defined a Downloadable as a program or document containing mobile code. Specifically, in the last Office Action response before allowance, the applicant explicitly stated that "[a]s is well known in the art, ***a Downloadable is mobile code*** that is requested by an ongoing process." JA233 (Response to Office Action at 6) (emphasis added). As such, because the patentee states a clear and unambiguous definition for this term, this construction and no other must prevail. *Scriptgen Pharm*, 79 F. Supp. 2d at 411.

In addition, during the prosecution of the '780 and '822 Patents, which are related to the '194 Patent, the patent applicant consistently referred to Downloadable as "mobile code." *See, e.g., Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1350 (Fed. Cir. 2004) (holding that statements made in prosecution of one patent are relevant to the scope of all sibling patents); *Watts v. XL Sys., Inc.*, 232 F.3d 877 (Fed. Cir. 2000) (a patent owner's limiting remarks, made during prosecution of the first patent, applied to a claim in the second patent because (1) the second patent was based on an application that was a continuation-in-part of the application upon which the first patent was based, (2) the second patent's claim had the same limitation "sealingly connected," and (3) the prosecution history of the second patent "contains nothing to the contrary."). For example, in the first Office Action response for the '780 Patent, a continuation patent claiming priority based on and having substantially the same specification as the '194 Patent, the patentee stated that "[t]he present invention concerns generation of an ID for ***mobile code downloaded to a client computer, referred to as a Downloadable***." JA410 (July 1, 2003 Response to Office Action at 7) (emphasis added).

This definition of "Downloadable" is also consistent with the language of the '822 Patent, which is a continuation-in-part application based on the '780 Patent. The '822 Patent provides that "[s]uch information can also include more traditionally viewed *'Downloadables' or 'mobile code'* (i.e. distributable components), as well as downloadable application programs or other further Downloadables, such as those that are discussed herein." JA53 ('822 Patent at 6:6-10)

(emphasis added). This excerpt from the '822 Patent demonstrates "Downloadable" means "mobile code" in the '194 Patent family according to the patent applicant. The applicant's clear intent must guide construction of this term as it is well-established in patent law that when "a patent applicant has elected to be a lexicographer by providing an explicit definition in the specification for a claim term … the definition selected by the patent applicant controls." *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). Indeed, based on the intrinsic evidence, this term could not be clearer; a "Downloadable" is a program or document containing mobile code.

Further, all three Finjan Patents refer to the same type of components when they refer to Downloadables or mobile code. For instance, the '194 and '780 Patents state that "[t]he Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script." JA13 ('194 Patent at 1:65-67); JA33 ('780 Patent at 2:5-6). Similarly, the '822 Patent provides:

> "Protection systems and methods provide for protecting one or more personal computers ("PCs") and/or other intermittently or persistently network accessible devices or processes from undesirable or otherwise malicious operations of Java™ applets, ActiveX™ controls, JavaScript™ scripts, Visual Basic scripts, add-ins, downloaded/uploaded programs or other 'Downloadables' or 'mobile code' in whole or part."

JA39 ('822 Patent, Abstract). As shown in these excerpts, all three Finjan Patents refer to Java applets, ActiveX controls, JavaScripts and Visual Basic scripts as both Downloadables and mobile code. Aside from the specific disclosures in the Patent specifications, one of ordinary skill in the art would know that these examples of Downloadables are also instances of mobile code. Consequently, the only proper construction of "Downloadable" is Finjan's definition of "program or document containing mobile code."

2. "addressed to a client"

Finjan's Construction	Secure Computing's Construction
Ordinary meaning within the context of the claims	addressed: containing the client computer's IP address client: the destination computer

The term "addressed to a client" requires no construction as it is easily understood by one skilled in the art in the context of the claim language. Claim 1 of the '194 Patent, which is representative of all claims asserted in the '194 Patent, recites this term in relevant part as follows: "[a] computer-based method, comprising the steps of: receiving an incoming Downloadable *addressed to a client*, by a server that serves as a gateway to the client...." JA17 ('194 Patent at 10:8-10) (emphasis added). One of ordinary skill in the art would recognize that this step is required of every network security system because a webpage that is sent to a client in a network is addressed to the client, no matter what component may relay the transmission. As such, the term "addressed to a client" requires no definition other than its ordinary meaning.

The parties apparently agree that the ordinary meaning applies, as Secure Computing's "construction" of this term seems to be no more than an elaborate paraphrasing of the term attached to arbitrary limitations. Specifically, Secure Computing proposes that the definition of "addressed to a client" should mean the client's IP address. Essentially, Secure Computing rearranges the words in hopes that the Court would improperly read in a limitation that requires the client's Internet Protocol ("IP") address.

In addition, the intrinsic evidence provides absolutely no support for this proposed limitation. Indeed, "IP address" or any variations thereof is not to be found anywhere in the Finjan Patents, demonstrating that the patentee had no intention of limiting the claim scope to a specific protocol. For example, a commonly known protocol is the Hypertext Transfer Protocol (HTTP) which is normally used to convey information between clients and servers. In addition to IP, HTTP can be used on top of any other protocol on the Internet or on other networks. The

claims are meant to cover HTTP because the invention provides security for web traffic.[3] However, under Secure Computing's construction, the claims would be improperly limited to one type of protocol.

To fully appreciate why reading in the "client computer's IP address" limitation into the claim is erroneous, one needs only to consider how network security generally works, as discussed above, and how the gateway serves to protect client. By way of example, when a webpage request is made, for security purposes, the gateway generally substitutes its IP address for the client's IP address to protect the client's identity.[4] Using this technique, the request appears as though it had come from the gateway. The response is then sent back to whoever requested the webpage. In this case, the response is sent to the gateway, using the IP address of the gateway, because it requested the webpage from the web server. At this point, the gateway will usually first analyze the content of the response for malicious content and then forward the content to the client by replacing its IP address with the client's IP address.

According to Secure Computing's construction, however, the gateway must first replace the IP address of the gateway with the IP address of the client before any analysis is performed. This is not efficient because there is no need to replace the IP address of the gateway if the webpage is going to be blocked and not sent to the client. In fact, the term "addressed to a client" indicates that the applicant did not intend to make a distinction between content that has the IP address of the client and content that has the IP address of the gateway.

Moreover, the claim language could not have been clearer that the crux of the matter is

---

[3] On the network layer alone, some alternative protocols include Internet Group Management Protocol (IGMP), Internet Control Message Protocol (ICMP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Routing Information Protocol (RIP), among others. Thus, it would be improper to limit the claims to any one protocol used in network security.

[4] For this example only, Finjan is using the IP address. However, as detailed above, any protocol that is able to covey information on a network can be used in a similar manner, and this example is not intended to limit the '194 Patent to only IP addresses.

that the gateway is to intercept the content of a request in the step for "receiving an incoming Downloadable addressed to a client, by a server that serves as a gateway to the client." *See* JA17 ('194 Patent at 10:9-10). The step is written broadly to include any file that is received by a gateway on its way to a client, regardless how the client is identified. For example, the '194 Patent specification states that the client can be identified as a member of a group or through a variety of interfaces. JA13-14 ('194 Patent at 1:67-2:6; 3:27-40). If the client is a member of a group or is identified through an interface, the client is not specifically identified, which means the client's address is not used. Nevertheless, the response is still addressed to the client because the client made the original request. As such, the term "addressed to a client" should be accorded its ordinary meaning within the context of the claim and requires no additional construction.

Further, the prosecution history supports Finjan's position that "addressed to a client" should be given its ordinary meaning. During the prosecution of the '194 Patent, the examiner and patent applicant corresponded regarding the "addressed to a client" term. In response to an Office Action mailed on January 7, 1999, the applicant amended the claims to cover a Downloadable that is received at the gateway by inserting the language "receiving an incoming Downloadable, addressed to a client, by a server that serves as a gateway to the client." The applicant made this amendment because in rejecting the claims, the examiner cited new art that utilized a gateway. Specifically, the examiner cited Boerbert and stated that "the purpose of this secure computer is to monitor all data exchanges and command requests between the public network and client." JA210 (June 17, 1999 Office Action at 3). In response, the applicant accepted the examiner's position that "receiving an incoming Downloadable, addressed to a client, by a server that serves as a gateway to the client" covers a secure computer that is used to monitor all data exchanges, and distinguish the invention on other grounds. JA231-32 (Oct. 27, 1999 Response to Office Action at 4-5). It is clear from this exchange that "addressed to a client" is a term well-known in the art and typically describes data that is exchanged between a public network and a client. Therefore, Finjan's construction should be adopted because it is

reflects the applicant's intent as evidence by the intrinsic evidence.

3. "server that serves as a gateway to the client"

Finjan's Construction	Secure Computing's Construction
Ordinary meaning within the context of the claims	a computer that receives data from its external communications interface and transfers the data through its internal communications interface to the client

The disputed term "server that serves as a gateway to the client" is found in every claim of the '194 Patent. The term is self-explanatory and does not require any further construction. As the term states, the claim discloses a server that acts as a gateway to the client. The server is referred to as a gateway because, much like a gate that stands between a house and the outside world, a server that acts as a gateway stands between the client and the Internet. In fact, most networks include a server that acts as a gateway in some fashion. As such, defining this term will only cause confusion and unnecessarily limit the scope of the claim.

The intrinsic evidence further supports Finjan's position that this term is well-known in the art and needs no construction. During the prosecution of the '194 Patent, the examiner stated that "Boerbert et al. discloses a system where a 'secure computer' (or gateway) stands between a client and a public network." JA210 (June 17, 1999 Office Action at 3). In response, the patentee agreed with the examiner's definition of "gateway" and distinguished the reference on other grounds. *See* JA231-32 (Oct. 27, 1999 Response to Office Action at 4-5). From this exchange, it is clear that a gateway is a commonly understood term in the art and refers to a server that stands between a client and a public network.

Secure Computing's proposed construction, on the other hand, attempts to improperly import limitations from one embodiment described in the '194 Patent specification. As the Federal Circuit has set forth in *Phillips*, "although the specification often describes very specific embodiments of the invention, [the Court has] repeatedly warned against confining the claims to those embodiments." *Phillips*, 415 F.3d at 1323. Disregarding the Federal Circuit's clear warning, Secure Computing attempts to improperly impose several limitations on a straightforward term, including "an external communication interface" and "an internal

communications interface" when the patent specifically discloses several alternative embodiments, including an integral interface. *See* JA14 ('194 Patent at 3:35-41). In contrast, Finjan's construction is correct in light of both the claim language and the prosecution history. As such, the Court should adopt Finjan's position.

C. Claim Interpretation of Finjan's '780 Patent

1. "performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID"

Finjan's Construction	Secure Computing's Construction
Ordinary meaning within the context of the claims	performing a hashing function on both the Downloadable and the fetched software components together to generate a single Downloadable ID

The term "performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID" is found in every claim of the '780 Patent. The claims of the '780 Patent are straightforward and disclose a method for generating a Downloadable ID. Thus, the only disputed term from this Patent requires no construction as it is well-understood in the art and should be accorded its ordinary meaning.

In fact, Secure Computing's construction shows that it agrees the ordinary meaning is sufficiently clear. The most persuasive evidence of this agreement is perhaps the following side-by-side comparison of the term and Secure Computing's "construction":

Claim Language	Secure Computing's Construction
performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID	performing a hashing function on **both** the Downloadable and the fetched software components **together** to generate a **single** Downloadable ID

As the chart illustrations, the only thing Secure Computing does to "construe" the term is to arbitrarily add three words– "both", "together" and "single" – in an attempt to unjustifiably limit the claim.

Obviously, Secure Computing largely agrees with the ordinary meaning but, without any

basis for doing so, adds three words that unnecessarily limit the claim language while introducing no clarification to the fact-finder. Indeed, Secure Computing's proposed construction is directly contradictory to the applicant's intent and use of the transitional phrase "comprising." By adding the words "both" and "together," Secure Computing attempts to restricts the claim to one hashing function that must be performed on the Downloadable and the fetched software component. Further, by adding the word "single" to the disputed term, Secure Computing attempts tot restricts the claim to only one Downloadable ID that can be generated from the hashing function. Secure Computing cannot improperly limit the scope of the claims, or the transitional phrase "comprising," by adding these restrictive words to the disputed term. As such, this term should be given its ordinary meaning.

D. Claim Interpretation of Finjan's '822 Patent

There are five contested terms in the '822 Patent, but only three require construction.

1. "downloadable-information"

Finjan's Construction	Secure Computing's Construction
program or document that can contain mobile code	data downloaded from one computer to another

The term "downloadable information" differs slightly from "Downloadable," used in the related '194 Patent. Whereas "Downloadable" means "program or document containing mobile code," "downloadable-information" should be construed as a "program or document that *can* contain mobile code". The reason that the construction of this term includes "can" is that the '822 Patent claim language sets forth an extra step to determine whether the downloadable-information is a Downloadable. *See* JA61 ('822 Patent at 21:11-27). To fully appreciate this requirement, one must consider the Finjan Patents in aggregate.

The Finjan Patents generally disclose methods and systems for protecting networks against malicious Downloadables. As described previously, the '194 Patent describes a method for analyzing and blocking a Downloadable at the gateway if it violates a security policy. While analyzing a Downloadable for malicious content, the '780 Patent further describes a method for

creating a Downloadable ID so that the system can recognize the Downloadable in the future. The '822 Patent, in turn, expands on the inventions disclosed in the '194 and the '780 Patents. Specifically, the '822 Patent discloses instances where a Downloadable does not violate the security policy, but *may* still be malicious because of the language it is written in, the Downloadable is wrapped in a sandbox before it is delivered to the client.

Finjan's construction of "downloadable-information" is the only construction consistent with the Finjan Patents and the intrinsic evidence. As stated in the specification, "downloadable-information" is a program or file that *can* contain mobile code. For example, the specification states in various parts that:

> "It is observed by this inventor, for example, that Downloadable information comprising program code can include distributable components (e.g. Java™ applets, JavaScript scripts, ActiveX™ controls, Visual Basic, add-ins and/or others)." JA51 ('822 Patent at 1:55-59).
>
> "Such [downloadable] information can also include traditionally viewed 'Downloadables' or 'mobile code' (i.e. distributable components)" JA53 ('822 Patent at 6:1-10).

A "Downloadable," on the other hand, is a program or file that *has* mobile code, as shown in the following examples:

> "In one aspect, embodiments of the invention provide for determining,…,whether received information includes executable code (and is a 'Downloadable.')" JA51 ('822 Patent at 2:37-42).
>
> "Thus, for convenience, received information will also be referred to as a 'potential-Downloadable,' and received information found to include executable code will be referred to as a 'Downloadable.'" JA55 ('822 Patent at 9:22-29).

As shown in the above excerpts, "downloadable-information" is a program or document that can contain mobile code. A "Downloadable," on the other hand, is a program or document that does contain mobile code. Because Finjan's construction is supported by the intrinsic evidence, its construction should be adopted by the Court.

Finjan's construction is also consistent with the other terms in the related Finjan Patents. The '194 and '780 Patents describe a Downloadable as a program or document that contains mobile code. The '822 Patent, on the other hand, discloses downloadable-information. Unlike a

Downloadable, downloadable-information is a program or document that can, but does not necessarily, contain mobile code. Due to this distinction, the '822 requires an additional step of checking the downloadable-information for executable, or mobile, code. *See* JA61 ('822 Patent at 21:13-14) ("determining whether the downloadable-information includes executable code"). Where the downloadable-information does contain mobile code, the program or document is deemed a Downloadable and mobile protection code is sent to the client. Therefore, the proper construction of "Downloadable" is "a program or document that contains mobile code" and the proper construction of "downloadable-information" is "a program or document that can contain mobile code." These constructions are consistent with each other, as well as meaningful in the context of the claim in which they appear.

2. "information-destination"

Finjan's Construction	Secure Computing's Construction
client	a device or process that is capable of receiving and initiating or otherwise hosting a mobile code execution

In general, the '822 Patent discloses a system set up in a client-server configuration. *See* JA53 ('822 Patent at 6:59-63). The '822 Patent specifically provides that "a simple client-server configuration will be presumed unless otherwise indicated." *Id.* ('822 Patent at 6:63-65). As such, an "information-destination" is a "client" where the client-server configuration is presumed to apply. Here, there is no indication that this default presumption is inapplicable.

Support for Finjan's construction is found throughout the '822 Patent specification. In various parts of the specification, "information-destination" is used interchangeably with "user device" and "client." For instance, the specification states that a client can be "a suitable information destination or 'user device.'" JA54 ('822 Patent at 7:60-64). In addition, the specification provides that "user devices 145 further includes a respective one or more clients...." *Id.* ('822 Patent at 7:39-42). In one section, the specification uses nearly identical language found in the claims of the '822 Patent to describe the system but substitutes "client" for "information-destination," as shown below:

> "4. A processor-based method, comprising: receiving downloadable-information; determining whether the downloadable-information includes executable code; and causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code, wherein the causing mobile protection code to be communicated comprises forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be communicated to the at least one information-destination." JA61 ('822 Patent at 21:35-48) (emphasis added).
>
> "A method according to an embodiment of the invention includes receiving downloadable information, determining whether the downloadable information includes executable code, and causing a mobile protection code and security policies to be communicated to a network client in conjunction with security policies and the downloadable information if the downloadable information is determined to include executable code." JA52 ('822 Patent at 3:41-48) (emphasis added).

Since "information-destination" is routinely used interchangeably with "client" in the specification, Finjan's definition is well supported by the intrinsic evidence and the only correct construction.

3. "information-recommunicator"

Finjan's Construction	Secure Computing's Construction
server	information supplier or intermediary for servicing one or more further interconnected devices or processes or interconnected levels of devices or processes

For much of the same reasons set forth above with regard to "information-destination," the proper construction of "information-recommunicator" is a "server." Again, the specification states that a client-server configuration is presumed unless otherwise indicated. *See* JA53 ('822 Patent at 6:63-65). Without any indication to the contrary, the presumed client-server configuration is applicable here.

Further, the specification consistently uses "information-recommunicator" and "server" interchangeably, thereby supporting Finjan's construction. For example, the specification explicitly provides that network connectable information re-communicating devices are referred to as servers or re-communicators. JA51 ('822 Patent at 2:56-60) ("or other network connectable *information re-communicating devices (as are referred to herein summarily one or more 'servers' or 're-communicators.'"*)) (emphasis added). In addition, the specification states that

the system can include "a protection-initiating host 'server' or 'recommunicator.'" JA54 ('822 Patent at 7:3-8). Thus, the specification uses these terms interchangeably. Finjan's construction of "information-recommuncator" is the proper construction because it finds substantial support in the intrinsic evidence.

4. "evaluating the detection indicators"

Finjan's Construction	Secure Computing's Construction
Ordinary meaning within the context of the claims	analyzing two or more detection indicators to determine whether executable code is detected

The meaning of "evaluating the detection indicators" is clearly set forth in the claim and does not require any further construction. The relevant portion of claim 1 recites:

> "wherein the determining comprises performing one or more analyses of the downloadable-information, the analyses producing detection-indicators indicating whether a correspondence is detected between a downloadable-information characteristic and at least one respective executable code characteristic, and evaluating the detection-indicators to determine whether the downloadable-information includes executable code." JA61 ('822 Patent at 21:20-27).

As set forth in claim 1, which is representative of all claims that contain this term, the detection indicators are a mechanism that alerts the system in the event the downloadable-information contains executable code. In other words, the detection-indicators indicate whether there is at least one correspondence between the downloadable-information and executable code. If so, the downloadable-information is deemed as a Downloadable.

Secure Computing's construction of "analyzing two or more detection indicators to determine whether executable code is detected," would render the claim nonsensical. As an initial matter, it makes little sense to produce two detection indicators as evidence of one correspondence between the downloadable information and executable code. In fact, a cursory reading of the plain language shows that "one or more analyses" in the claim refer to one or more detector indicators, not two or more detection indicators. Applying the proper rules of English to the claim language, one analysis would produce one detection indicator to indicate a single correspondence between the downloadable information and executable code. Consequently,

Secure Computing's construction should be rejected because it renders the invention non-functional.

Additionally, the intrinsic evidence does not provide any support for Secure Computing's construction. In fact, the intrinsic evidence directly contradicts this definition. First, the specification does not require that there be two detector indicators. On the contrary, the specification provides that there only needs to be one or more detection indicators, as illustrated below:

> "Agent generator 431 includes an MPC generator 432 and a protection policy generator 433 for 'generating' an MPC and a protection policy (or set of policies) respectively upon receiving one or more 'generate MPC/policy' indicators from detection engine 402, indicating that a potential-Downloadable is a detected-Downloadable." JA56 ('822 Patent at 12:56-61).
>
> "As shown, one or more aspects can provide useful indicators of the inclusion of executable code within the potential-Downloadable." JA60 ('822 Patent at 19:43-44).

In fact, there is no reference whatsoever in the specification to "two or more" detection indicators. Since there is no support for Secure Computing's construction, it should be rejected, and the term should be given its ordinary meaning.

5. "level of downloadable-information characteristic and executable code characteristic correspondence"

Finjan's Construction	Secure Computing's Construction
Ordinary meaning within the context of the claims	a value representing the degree of correspondence between the downloadable-information characteristic and the executable code characteristic

"Level of downloadable-information characteristic and executable characteristic correspondence" is a simple term that makes perfect sense in the context of the claim. As such, this term requires no construction and should be given its ordinary meaning within the context of the claim language.

This term is found in the dependent claims 2 and 10 of the '822 Patent and refers to the detection indicators discussed above. *See* JA61 ('822 Patent, claims 2 and 10) ("the method of claim 1, wherein at least one of the detection-indicators indicates a level of downloadable-

information characteristic and executable code characteristic correspondence"). As set forth above, the detection indicators show whether a correspondence exists between the downloadable-information and executable code in order to determine if the downloadable-information is a Downloadable (a program or document that actually contains executable, or mobile, code). The purpose of dependent claims 2 and 10 is to illustrate a specific function of the indicators which is the level, or how much, the downloadable-information corresponds to executable code. If the level of correspondence meets a sufficient threshold, the downloadable-information is determined to be a Downloadable and mobile protection code is communicated to the client. If the level is not reached, the downloadable-information is not considered to be a Downloadable and no further processing is required. This functionality is apparent from the plain language of the independent and dependent claims and therefore, this term requires no further construction. *See, generally*, JA60 ('822 Patent at 19:40-20:3).

Secure Computing's proposed construction is arbitrary and should be disregarded. Specifically, the intrinsic evidence provides no support for essentially defining "level" as "a value representing the degree of correspondence." In fact, "value" and "degree of correspondence" are not found anywhere in the specification. Because no support exists for Secure Computing's construction, it should be rejected and the term should be given its ordinary meaning.

E. Claim Interpretation of Secure Computing's '010 Patent

The '010 Patent is a very specific patent that includes four terms that require construction.

1. "document control server"

Finjan's Construction	Secure Computing's Construction
a mechanism which allows a specified business partner to access documents on another company's non-public internal network	Ordinary meaning within context of the claim

As described in the '010 Patent, "document control server" describes a particular type of server. The '010 Patent is limited to, as the title suggests, a "System and Method for Controlling

Access to Documents Stored on an Internal Network." In addition, "document control server" is a technical term that cannot be understood by reading only the claim language. As such, the Court must look to other intrinsic evidence for this construction. *Multiform Desiccants*, 133 F.3d at 1478 ("The best source for understanding a technical term is the specification from which it arose, informed, as needed, by the prosecution history.")

In general terms, the '010 Patent discloses a document control system that allows users access to a company's non-public internal network. *See, generally*, JA63 ('010 Patent, Abstract). Even in the very first line of the Abstract, the '010 Patent describes "[a] system and method of limiting access from an external network to documents stored on an internal network." *Id.* This characterization is consistently reiterated throughout the specification. For example, the first line of the Summary of the Invention states that:

> "The present invention is a system and method of limiting access from an external network to documents stored on an internal network." JA72 ('010 Patent at 1:66-2:1).

Again, the Description of the Preferred Embodiments provides that:

> "The present invention solves this problem by allowing specified external users controlled, customized, and secure access to the company's intranet without complex network infrastructure modifications." JA73 ('010 Patent at 3:6-9).

The clear intent of the '010 Patent is to describe a system that allows business partners access to a company's non-public internal network. Since Finjan's construction plainly reflects this intent, its construction should be adopted.

In addition to a stated general objective, the '010 Patent specifically states that the document control server provides the primary functionality of the invention. For instance, the specification provides that:

> "Document control server 12 offers several advantages over current methods such as cost savings, improved customer service and leveraging of the current infrastructure. Current methods for passing data to outside partners are expensive, slow and unreliable. Document control server 12 offers the information to partners faster, easier and cheaper. It also more tightly integrates partners, thus improving business relations. Document control server 12 also leverages the benefits of current technology such as the Internet and Intranet." JA79 ('010 Patent at 16:1-10).
>
> "Other business advantages of document control server 12 include: it reduces overhead and costs; it eliminates the need to copy content to a web server within the DMZ or

> external network; it offers spontaneous, dynamic user-managed content; it eliminates the wait for an IS manager to update data or post on a web server; it eliminates integrity and replication issues; it more tightly integrates partners; and its open architecture allows access without the need to alter current technology." *Id.* ('010 Patent at 16:11-19).

The document control server provides these advantages because it provides business partners with access to internal documents, as illustrated by the following excerpts from the '010 Patent:

> "Document control server 12 enables users to easily, but accountably, grant authenticated partner access to internal web data, with complete control and authorization. Outside partners need only access a predefined URL in order to access an internal web page." JA78 ('010 Patent at 14:63-67).

> "In operation, the document control sever receives a document request from the external interface for the first document, determines a user associated with the document request, authenticates the user, determines if the user has authorization to access said first document and, if authorized, reads the first document from the document server, cleans the first document and forwards a clean version said first document to the user." JA72 ('010 Patent at 2:23-30).

> "[The document control system] is essentially a secure window through which outside partners can view internal web data." JA74 ('010 Patent at 6:8-9).

In addition, it is clear that the user of the document control sever is a business partner. In fact, the only kind of user described in the '010 Patent is an external business partner. The following quotes from the '010 Patent are exemplary:

> "When an external business partner (user) enters the URL,…." JA73 ('010 Patent at 4:44).

> "The term 'Business Partner' is used in the following discussion to describe an external user who needs access to data such as Web pages which are not generally available to the public, but who also should not have unlimited [access] to a company's intranet Web services." *Id.* ('010 Patent at 3:12-16).

> "When document control server 12 passes an outside partner to any Intranet URL, the user is authenticated as a unique document control server 12 user, however, that user ID is not passed on to the Intranet server." JA78 ('010 Patent at 13:16-19).

As illustrated in the above citations, the document control server is the focus of the '010 Patent. The alleged novelty of the document control server lies in its ability to allow external business partners access to a company's non-public internal network. As such, "document control server" should be construed as "a mechanism which allows a specified business partner to access documents on another company's non-public internal network."

2. "fetching the requested document"

Finjan's Construction	Secure Computing's Construction
obtaining, parsing, and cleaning the document	Ordinary meaning within context of the claim

The term "fetching the requested document" should be defined as "obtaining, parsing and cleaning the document" because the patentee's intent, as it is reflected by the specification, indicates that the obtaining, parsing and cleaning of the document are all necessarily a part of the fetching act. Indeed, the '010 Patent specification provides that "once the internal connection has been made, document control server must parse and 'clean' the Web page prior to returning it to the requesting user." JA73 ('010 Patent at 3:51-53). In addition, the claim language describes a process where a document control system receive a request for a document, determines whether the user associated with the request has permission to access the document, and fetching and sending the document to the user if it is determined that the user has such permission. *See, generally*, JA79-80 ('010 Patent at 16:29-44, 17:3-19). Specifically, some of the claims explicitly provide that, in the event the user has permission to access the document, the document control system first obtains, parses, and cleans the document before forwarding it onto the user. *See* JA80 ('010 Patent at 17:3-19; 18:51-56) (claim 7 provides "reading the first document from the document server, cleaning the first document and forwarding a clean version of said first document," claim 23 states "if the user associated with the document request has permission to access the document requested, retrieving the document requested from the internal network, cleaning the document of embedded links and delivering the document to the user associated with the document request."). In other claims describing the same process but not explicitly set out these steps, a "fetching" step is used where the obtaining, parsing, and cleaning steps would otherwise be expected. *See* JA79 ('010 Patent at 16:42-44) (claim 1 provides "if the requested document is on the list of documents, fetching the requested document as a proxy and sending the requested document to the client."). As such, the appropriate construction of "fetching the requested document" is "obtaining, parsing, and cleaning the

document," because the intrinsic evidence indicates that the obtaining, parsing, and cleaning constitute necessary steps in the fetching act.

3. "proxy"

Finjan's Construction	Secure Computing's Construction
a process performed by a firewall in which the actual destination on the internal network is hidden from the business partner who is requesting the connection from an external network	Ordinary meaning within context of the claim

"Proxy" is a general and broad term with no ordinary meaning within the context of the '010 Patent claims. As such, "proxy" means "a process performed by a firewall in which the actual destination on the internal network is hidden from the business partner who is requesting the connection from an external network," a definition that is consistent with the intrinsic evidence. *Kinik*, 362 F.3d at1365 ("The words of patent claims have the meaning and scope with which they are used in the specification and the prosecution history.").

The specification of the '010 Patent discusses two types of proxies, both of which fall within Finjan's construction. As stated above, the '010 Patent is directed to allowing external business partners access to a company's non-public internal network. In order to provide additional security to the internal network, a proxy may be used. *See* JA78 ('010 Patent at 13:51-67).

The first type of proxy described in the specification is a redirected proxy. *See id.* ('010 Patent at 13:51-67). Within the context of the '010 Patent, a redirected proxy is a process set up on a firewall to reroute the connection from the external business partner in order to hide the actual destination to which the business partner's request will be sent. *See id.* In addition to the redirected proxy, the '010 Patent also discloses a transparent proxy. *See id.* A transparent proxy is a process set up through a firewall that creates the illusion that a business partner is connecting directly to an internal server, rather than through the firewall. *See id.* In either case, the proxy hides the actual destination from the business partner who is requesting the connection. *See id.*

As such, Finjan's construction, which is fully supported by the intrinsic evidence, should be adopted.

4. "role"

Finjan's Construction	Secure Computing's Construction
an alias which provides access to a list of allowed documents	membership in a group of one or more

Finjan's construction of "role" as "an alias which provides access to a list of allowed documents," is wholly consistent with the '010 Patent specification and therefore should be adopted by the Court. Within the context of the '010 Patent, "role" has a specific technical meaning and, as such, its construction must be based on a reading go the intrinsic evidence. *Metabolite Labs.*, 370 F.3d at 1360 ("In most cases, the best source for discerning the proper context of claim terms is the patent specification wherein the patent applicant describes the invention. In addition to providing contemporaneous technological context for defining claim terms, the patent applicant may also define a claim term in the specification 'in a manner inconsistent with its ordinary meaning.'")

The specification of the '010 Patent states that "each role has access to a set of allowed URLs associated with that role." JA73 ('010 Patent at 4:14-19); *see also* JA953, JA963 (Sept. 19, 2000 Response to Office Action at 6 and 16). In addition, the specification provides that "an owner is assigned to one or more 'roles,' where a 'role' represents a mapping alias assigned to one of the servers." JA74 ('010 Patent at 6:50-54). Consistent with the intrinsic evidence, Finjan's construction incorporates both functions of a "role" and, as such, should be adopted.

F. Claim Interpretation of Secure Computing's '361 Patent

At the outset, all references to a "protocol" in the '361 Patent claims should be limited to a lightweight directory access protocol (LDAP). The '361 Patent is directed, as the title indicates, to a "System, Method and Computer Program Product for Authenticating Users Using a Lightweight Directory Access Protocol (LDAP) directory server." Generally, an LDAP is a protocol for storing and retrieving documents from a database or directory. Further, the only

embodiments described in the '361 Patent are systems that utilize the LDAP. *See, generally,* JA90-93 ('361 Patent at 1:9-7:16, which describes two embodiments one using per-user authorization scheme and one using a per-service authorization scheme, both using LDAP). Since the LDAP is the only protocol referred to throughout the intrinsic evidence, the claims should be limited accordingly. *Iredeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1303 (Fed. Cir. 2004) (holding a claim term is limited to a narrower construction when every example in the specification depicts the same embodiment); *see also Bell Atlantic Network Servs., Inc. v. Covad Communs. Group, Inc.*, 262 F.3d 1258, 1271 (Fed. Cir. 2001) ("Thus, when a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term 'by implication'.") (citations omitted).

The '361 Patent contains a number of disputed terms because the nature of the intrinsic evidence imposes inherent limitations to the claims. Accordingly, seven terms are in dispute.

1. "firewall"

Finjan's Construction	Secure Computing's Construction
firewall that does not authenticate users using its own database but, rather, information contained within an LDAP directory	Ordinary meaning within context of the claim

The '361 Patent claims a specific type of firewall. Generally, a firewall is a mechanism that allows only authorized users to access a network using its own authentication database. The patentee here clearly disclaimed the ordinary meaning for the term "firewall" within the context of the '361 Patent. Specifically, the '361 Patent provides that "in accordance with the present invention, firewall 210 does not authenticate users using its own database. Rather, firewall 210 authenticates users using information contained within LDAP directory 204." JA91 ('361 Patent at 4:41-44). In addition, the applicant admits in the '361 Patent that prior art firewalls are configured with their own authentication database:

> "Conventional firewalls 110 included their own database having a list of users and passwords, to enable authentication through firewall 110." *Id.* ('361 Patent at 4:38-40).
>
> "Firewalls also maintain a database of users and are operative to prompt users for an

identifying user identifier and password. These conventional firewalls require that employee names and passwords be entered into a firewall authentication database." JA90 ('361 Patent at 2:53-57).

Since the '361 Patent specification clearly disavows a firewall that authenticates users using its own database, the ordinary meaning does not apply. It is well-settled in patent law that "the specification may reveal an intentional disclaimer, or disavowal, of claim scope by the inventor." *Phillips,* 415 F.3d at 1316. Accordingly, the patentee's intent is dispositive. Since the patentee here obviously contemplated a firewall that works exclusively with a LDAP directory, Finjan's construction should be adopted by this Court.

2. "a server having at least one directory that can be accessed using a network protocol"

Finjan's Construction	Secure Computing's Construction
an internal server having an LDAP directory that stores information about users, offers a static view of information and allows simple updates without transactions	Ordinary meaning within context of the claim

Finjan's construction of this term is consistent with the intrinsic evidence and provides clarity to the fact-finder. In describing a server, the '361 Patent specification provides that "internal server 106 is shown including a lightweight directory access protocol (LDAP) directory 204, which can be configured to store employee information." JA91 ('361 Patent at 4:17-19). More specifically, the patentee defines a "directory" as a database that "can store information about users" and "offers a static view of information and allows simple updates without transactions." JA90 ('361 Patent at 2:18-27). In addition, the '361 Patent points out the flaws of using traditional directory services for authentication purposes, discloses a new protocol known as LDAP, and proceeds to explicitly state that "what is needed is a mechanism for leveraging an existing LDAP directory server as part of a firewall's authentication process." *Id.* ('361 Patent at 2:33-67). As such, Finjan's straightforward and clear construction closely tracks the patentee's own definitions for the subparts of this term, finds substantially support in the intrinsic evidence, and, therefore, should be adopted.

3. "authorization filter"

Finjan's Construction	Secure Computing's Construction
a module to determine whether one or more attributes of the client user's LDAP entry is satisfied or whether the client user is a member of a group in the LDAP directory	Ordinary meaning within context of the claim

An "authorization filter" is a tailored to convey a specific technical meaning and consequently has no ordinary meaning outside the '361 Patent. In addition, it is well established that "a word describing patented technology takes its definition from the context in which it was used by the inventor…[and] the term cannot be defined by some ordinary meaning isolated from the proper [technical] context."). *Tap Pharm. Prods., Inc. v. Owl Pharms., L.L.C.*, 419 F.3d 1346, 1354 (Fed. Cir. 2005). As such, this term requires a construction consistent with the intrinsic evidence.

The '361 Patent discloses two instances where an authorization filter is used. The first is within the context of determining "whether one or more attributes of the client user's LDAP entry satisfies an authorization filter." JA92 ('361 Patent at 5:25-27); *see also* JA1108 (Jan. 12, 2004 Response to Office Action at 8); JA1137-38, JA1142 (Feb. 28, 2005 Appellant's Brief on Appeal at 7, 8, and 12). A second instance where the term appears discloses that, "to satisfy this authorization process, the authenticated user must be a member of the 'web-users' group in the LDAP directory." JA92 ('361 Patent at 6:43-45). As such, Finjan's construction encompasses both functions of an "authorization filter" and should be adopted by the Court.

4. "directory schema that is predefined by said entity"

Finjan's Construction	Secure Computing's Construction
an authentication scheme specified to interact with an existing LDAP directory that has been uniquely developed for an organization's internal needs	Ordinary meaning within context of the claim

The term "directory schema that is predefined by said entity" is found in every claim of the '361 Patent. Specifically, independent claims 1, 8, and 15 use the term to describe generating an authorization filter "based on a directory schema that is predefined by said entity." JA93

('361 Patent at 7:30-31, 52-55; 8:41-44).

The '361 Patent specification summarily describes a feature in which an authentication scheme can be "configured independently of specially stated field requirements or schema of the firewall," by flexibly specifying the scheme "to interact with a LDAP directory that has been uniquely developed for a company/organization's internal needs." JA91 ('361 Patent at 3:11-18; 4:48-59). The claims of the '361 Patent, in turn, disclose using a directory to "store information concerning an entity's organization," wherein the directory is a LDAP directory. JA93 ('361 Patent at 7:21-23, 32-35, 50-51; 8:7-10, 38-40). In addition, the claims state that the entity predefines a directory schema for generating an authorization filter, which is in turn used in a comparison to the content of the directory's entries. JA93 ('361 Patent at 7:24-31, 49-55; 8:38-44). In other words, the claims contemplate a LDAP directory adapted to store information related to an entity's organization and a directory schema that is predefined by the entity in order to interact with the LDAP directory. As such, when read in light of the '361 specification, Finjan's construction of this term as "an authentication scheme specified to interact with an existing LDAP directory that has been uniquely developed for an organization's internal needs" is the only correct interpretation.

Secure Computing, on the other hand, reiterates its contention that the fact-finder needs only read the term within the context of the claim language to understand it. The claims, however, only provide "wherein said authorization filter is generated based on a directory schema that is predefined by said entity." *Id.* ('361 Patent at 7:30-31, 52-55; 8:41-44). Since Secure Computing refuses to provide any lay definition and insists that both "authorization filter" and "directory schema that is predefined by said entity" need no construction, its arbitrary conclusion that ordinary meaning would suffice leaves the fact-finder without any means to understand the claims. As such, the Court should adopt Finjan's construction for "directory schema that is predefined by said entity."

5. "network protocol"

Finjan's Construction	Secure Computing's Construction
lightweight directory access protocol	Ordinary meaning within context of the claim

"Network protocol" appears in all the claims of the '361 Patent. Finjan's construction of this term as "lightweight directory access protocol" is firmly rooted in the '361 Patent. The Patent is directed specifically to a "System, Method and Computer Program Product for Authenticating Users Using a Lightweight Directory Access Protocol (LDAP) Directory." JA90 ('361 Patent at 1:1-5). The only network protocol disclosed in the intrinsic evidence is a LDAP. In addition, the only instance where this term appears in the specification refers to "network protocol" as defined by a LDAP standard for the purposes of accessing information in the LDAP directory. *Id.* ('361 Patent at 2:39-43). In fact, every description of any network protocol is specifically directed to a LDAP. *See, e.g.*, JA86, JA88-89, JA91-92 ('361 Patent at 3:3-6, 14-17; 4:17-27, 41-47; 5:9-41; 6:24-26, 64-65; Figs 2, 4, and 5). Similarly, the claim language discloses a network protocol for accessing a directory wherein the directory is a LDAP directory. JA93 ('361 Patent at 7:20-23, 32-35, 49-51; 8:7-10, 38-40). The Court should adopt Finjan's construction for this term because it is the only definition that is supported by the '361 Patent specification and claim language.

6. "per-service authorization scheme"

Finjan's Construction	Secure Computing's Construction
a scheme in which the authorization module determines whether the user is in one or more groups in the LDAP directory in order to satisfy the authorization filter	Ordinary meaning within context of the claim

The term "per-service authorization scheme" appears in claims 5 and 12 in the context of "said authorization filter implements a per-service authentication scheme." JA93 ('361 Patent at 7:38-39; 8:18-20).

The '361 Patent states that an authorization process can be based on a per-service basis. JA92 ('361 Patent at 6:33-35). Specifically, the '361 Patent describes the per-service authorization process as one where a user's membership in one or more groups in a LDAP

directory is the determining factor for whether the user gains access to particular requested services. *Id.* ('361 Patent at 6:40-45, 53-63). The '361 Patent claim language, when read in light of the specification, clearly discloses an authorization filter that allows or denies a user access to services according to the user's membership in one or more LDAP directory.

Contrary to Secure Computing's contention, the claim language merely states that the authorization filter implements a per-service scheme without clarifying what the scheme entails. It is unclear how the word "per-service" would alert the reader to the fact that the deciding factor is the *user*'s membership in one or more groups in a LDAP directory.

7. "per-user authentication scheme"

Finjan's Construction	Secure Computing's Construction
a scheme in which the authorization module determines whether one or more attributes of the client user's LDAP entry satisfies the authorization filter	Ordinary meaning within context of the claim

The term "per-user authorization scheme" appears in claims 4 and 11 in the context of "said authorization filter implements a per-user authentication scheme." JA93 ('361 Patent at 7:36-37; 8:15-17).

Without any qualification, the '361 Patent states that where per-user authorization is configured, an authorization module "determines whether one or more attributes of the client user's LDAP entry satisfied an authorization filter." JA92 ('361 Patent at 5:25-27). Finjan's construction tracks this language almost verbatim. Moreover, similar to "per-service authorization scheme," the claim language provides no guidance what criteria a "per-user authorization scheme" is based on. As such, the Court should adopt Finjan's construction because it is the only interpretation supported by the intrinsic evidence.

IV. CONCLUSION

For the foregoing reasons, Finjan respectfully requests that the Court adopt its proposed constructions for the disputed terms discussed above.

POTTER ANDERSON & CORROON LLP

By: _____

Philip A. Rovner (#3215)
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(303) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

OF COUNSEL

Paul J. Andre
Lisa Kobialka
Meghan A. Wharton
James R. Hannah
Perkins Coie LLP
101 Jefferson Drive
Menlo Park, CA 94025-1114
(650) 838-4300

Dated: September 7, 2007
817659

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on September 7, 2007, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

BY HAND DELIVERY AND E-MAIL

Frederick L. Cottrell, III, Esq.
Kelly E. Farnan, Esq.
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
cottrell@rlf.com; farnan@rlf.com

I hereby certify that on September 7, 2007 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.
Christopher A. Seidl, Esq.
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
jmholdreith@rkmc.com ; caseidl@rkmc.com

Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P.O. Box 951
Wilmington, Delaware 19899
(302) 984-6000
E-mail: provner@potteranderson.com